USAWC STRATEGY RESEARCH PROJECT

EVALUATION OF INFORMATION ASSURANCE REQUIREMENTS IN A NET-CENTRIC ARMY

by

Colonel Scot Miller
United States Army

Professor Robert Coon
Project Adviser

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
18 MAR 2005		**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Evaluation of Information Assurance Requirements in a Net-Centric Army	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Scot Miller	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**30**	

ABSTRACT

AUTHOR: Colonel Scot Miller

TITLE: Evaluation of Information Assurance Requirements in a Net-Centric Army

FORMAT: Strategy Research Project

DATE: 18 March 2005 PAGES: 30 CLASSIFICATION: Unclassified

Network centric capabilities are a key enabler for the transformational army and planned employment of Units of Action in the future. Information Assurance refers to the security and assurance of the information that is being passed within the myriad networked systems at multiple data rates and security classifications. This paper will examine the requirements and concurrent capabilities necessary for this key strategic imperative of future Army operations as part of a joint and coalition force.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

For DQ, P-Miller, and Jake – thank you for your unwavering and unconditional support and to COL(R) Gary Kosmider – keep hanging in there, Pop.

EVALUATION OF INFORMATION ASSURANCE REQUIREMENTS IN A NET-CENTRIC ARMY

Based on current and emerging doctrine for the Department of Defense (DoD), network centric warfare capabilities will be a key enabler for the transformational army and planned employment of Units of Action (UAs) in the future. These capabilities will assist in greatly increasing the common operational picture, or more correctly, the common operational understanding, of all players within the networked battle-space. They will also allow the networked commander or decision maker to stay within the adversary's decision cycle through the inherent availability of more accurate and timely information.

Information Assurance (IA) refers to the security and fidelity of the information that is being passed within the myriad networked systems at multiple data rates and security classifications. It is an explicit expectation and imperative for warfighting forces that the information being passed within the supporting Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems will be secure and uncompromised.

This paper will examine the requirements and concurrent capabilities necessary for this crucial strategic imperative of future Army operations as part of a joint and coalition force. It will begin by describing Network Centric Warfare (NCW) and Network Centric Operations (NCO) and their importance and place within the Army's and DoD's operational concepts. It will then discuss information assurance requirements within the global C4ISR construct, look at some of the unique considerations of information assurance with respect to network centricity, and the implications of those concepts within the broader context of the National Security Strategy (NSS) and National Military Strategy (NMS). Finally, it will assess some of the key challenges with regard to information assurance of network centric systems and capabilities, with specific regards to the Army's Future Force, and provide recommendations for mitigation strategies to address these potential challenges.

NETWORK CENTRIC WARFARE – A BRIEF TUTORIAL

> …we must achieve: fundamentally joint, network-centric, distributed forces capable of rapid decision superiority and massed effects across the battlespace. Realizing these capabilities will require transforming our people, processes, and military forces.[1]
>
> - Secretary of Defense Donald Rumsfeld

Network centric warfare and its kinder, gentler twin, network centric operations, are products of the information age and the commensurate increases in computing power as well as

standardization of interfaces, protocols, and applications to take advantage of these technological advancements. A reasonable definition of NCW is provided by David Alberts, John Gartska, and Fred Stein in *Network Centric Warfare: Developing and Leveraging Information Superiority."* Here, NCW is defined as, "An information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization."[2] In this context, information superiority is considered in the context offered by Army Vision 2010, which defines it as, "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[3] This definition implies that information sharing across the full continuum of operations enables a variety of capabilities that were here-to-fore not available to the warfighter or decision-maker. Thus, the power of NCW is not so much in the network, but more in the ability to share information through the power of networking.[4]

The power of networking has most vividly been demonstrated in the development and growth of the Internet. The ubiquitous and pervasive nature of this technology in an information craving society illuminates the potential of networks and the information and knowledge sharing they perpetuate. Roger Roberts, in a speech on network centric operations given at the 2003 Network Centric Operations Conference, indicates that the value of the Internet is that it acts like "a living entity that is constantly receiving new data, cataloging it, and storing it so that those in search can find the most up-to-date information easily and quickly."[5] He then extrapolates that logic to warfighting utility by suggesting that NCW concepts provide ways to "use the power of the network to access information from far reaching resources in order to make timely, effective, and sometimes life saving decisions."[6] Thus, the power of networking, and NCW in general, is in the ability to share information, and more importantly knowledge, across the full spectrum of operations, from the strategic to the tactical level.

To expand on this further, the 2001 DoD Network Centric Warfare Report to Congress highlighted four tenets of Net-Centric Warfare and their applicability to the enhancement of warfighting capability:

- A robustly networked force improves information sharing
- Information sharing enhances the quality of information and shared situational awareness
- Shared situational awareness enables collaboration and self-synchronization
- These, in turn, dramatically increase mission effectiveness[7]

As noted above, networking and networked systems do not inherently provide a competitive advantage to the operational or tactical decision-maker. It is only through the collaboration and synchronization of processed information that information superiority begins to turn into "decision superiority" and the power of network centricity is fully realized. JV 2020 defines decision superiority as "better decisions arrived at and implemented faster than an opponent can react, or in a non-combat situation, at a tempo that allows a force to shape the situation or react to changes and accomplish its mission."[8] "Network centric warfare is no less than the embodiment of Defense Department transformation. It will increase warfighting capabilities more than all the advances that have been made in the history of warfare to date."[9] Indeed, network centricity and network centric operations are vital to the realization of joint transformation capability and central to Joint Operations Concepts (JOpsC).

NCO AND THE JOPSC

The JOpsC "describes how the Joint Force intends to operate in the next 15 to 20 years" and "provides the operational context for the transformation of the Armed Forces of the United States by linking strategic guidance with the integrated application of Joint Force capabilities."[10] Three of the eight common core capabilities described in the JOpsC are directly dependent on NCO and NCW - achieve common understanding of all dimensions of the battlespace throughout the joint force; make joint decisions and take action throughout the joint force faster than the opponent; and adapt in scope, scale, and method as the situation requires.[11] To realize the common core capabilities, the JOpsC describes seven fundamental attributes that the future Joint Force must possess, one of which is specifically network-centric focused and four of which (also bolded) are directly tied to and dependent upon NCO - **Fully Integrated**, Expeditionary, **Networked**, **Decision Superior**, **Adaptable**, **Decentralized**, and Lethal.[12] The JOpsC considers how NCO enables joint operations in the following manner, "Networked joint forces will increase operational effectiveness by allowing dispersed forces to more efficiently communicate, maneuver, share a common operating picture and achieve the desired end-state."[13] It goes on to highlight that, "A networked Joint Force is able to maintain a more accurate presentation of the battlespace built on the ability to integrate intelligence, surveillance and reconnaissance, information and total asset visibility. This integrated picture allows the Joint Force Commander (JFC) to better employ the right capabilities, at the right place and at the right time. Fully networked forces are better able to conduct distributed operations."[14]

ENABLING EFFECTS BASED OPERATIONS

Ultimately, the power of NCW to Joint and Coalition operations, as well as the transformational army, is its ability to allow the decision-maker to get inside the opponent's decision cycle and to bring the right effects to bear at the right time, a realization of effects-based operations. Effects-based operations are defined in *Military Transformation: A Strategic Approach* as "primarily about focusing knowledge, precision, speed, and agility on the enemy decision-makers to degrade their ability to take coherent action…"[15] and is not necessarily focused on the physical destruction of the enemy, but strives to "induce an opponent or an ally or a neutral to pursue a course of action consistent with our security interests."[16] It is useful to examine the relationship between these two constructs and their application to U.S. Army Future Force concepts and operations.

IT'S THE NETWORK, STUPID

> Transforming our Nation's military capabilities while at war requires a careful balance between sustaining and enhancing the capabilities of current forces to fight wars and win the peace while investing in the capabilities and experimentation, science and technology (S&T) investment, and future force design that enables interdependent network-centic warfare will ensure future capabilities meet the requirements of tomorrow's Joint Force.[17]
>
> - Forward, 2003 Army Transformation Roadmap

The Army's Future Combat System (FCS) and its operational implementation within brigade-sized UAs rely heavily on network centric capabilities. The FCS is the Army's "multifunctional, multimission, reconfigurable family of systems (FoS) designed to maximize joint interoperability, strategic transportability, and commonality of mission roles."[18] The FCS will serve as the cornerstone for Army Future Force UAs and is comprised of 18 manned and unmanned platforms anchored by a 19th element, the Soldier, and integrated with a 20th component, the battle command network.[19] This construct has come to be referred to as the 18+1+1 concept to emphasize its focus on the soldier as a system that is enabled by this collection of highly capable sensors, platforms, and capabilities and fully interconnected by the network to achieve the desired situational understanding of the battlespace at the lowest tactical level.

The FoS approach embraces a diverse mixture of capabilities to achieve this full-spectrum battlespace awareness. Figure 1 illustrates the elements that comprise the FCS FoS. Unmanned platforms include multiple Unmanned Air Vehicle (UAV) variants, Unmanned Ground Vehicles (UGVs), Unattended Ground Sensors (UGS), both Loitering Attack Munitions and

Precision Attack Munitions (LAMs/PAMs), Intelligent Munitions Systems (IMS), and the Non-line-of-Sight Launch System (NLOS-LS). The manned systems consist of a family of common vehicles that comprise the eight manned ground vehicle variants.

FIGURE 1. ELEMENTS OF THE FUTURE COMBAT SYSTEM FAMILY OF SYSTEMS.

All of these platforms have significant potential to provide battlespace awareness and contribute to decision superiority across the full spectrum of operations, but truly are just a collection of impressive, shiny-new autonomous combat systems or enablers without the final jewel in the crown – the network. When asked what the most important system was within the FCS program, a senior Army official associated with the FCS program illustrated this point and underlined its importance to the effectiveness of envisioned FCS capabilities, by stating, "It's the Network, Stupid."[20] These words have been a mantra for the FCS community over the past two years to emphasize the importance of the network function to the success of future force concepts and operations. Without this connectivity, and the knowledge and assurance of the fidelity of the data being shared amongst the collective constituents, the full promise of information-age and transformational capabilities simply will not be realized.

NOT YOUR FATHER'S COMMAND, CONTROL, AND COMMUNICATIONS

A key feature of network centric operations is how it changes the landscape of battlefield communications. Command, control, and communications (C3) doctrine, even as recently as Operations Enduring and Iraqi Freedom (OEF & OIF), involved the use of dedicated communications systems and platforms that tied multiple, relatively large, communications nodes together over the area of operations. In most cases, these nodes require several vehicles, have a significant geographic footprint, and present an attractive and easily identifiable target to our adversaries. Additionally, they require an inordinate amount of time to move and emplace, and are not sufficiently mobile and agile to support the speed and tempo of maneuver force operations today and in the future.

Network centric concepts move away from this nodal-based approach to a distributed methodology that pushes more of the communications and network capability to the individual elements comprising the network. The distributed nature of networked forces provides the desired and necessary flexibility, robustness, speed of command, and shared awareness of the battlespace that future force elements desire, and indeed, will require. Additionally, as the JOpsC points out, the network attribute is key not only to joint combat forces, but also to the joint combat support and service support functions that enable the joint maneuver force. Accordingly, NCO and the effects-based approach to warfare that it enables work hand-in-hand from the tactical to strategic levels as ways to achieve our national ends. However, the inherent power that is derived from the networking of all the elements in the system also means that there are more elements that can potentially be exploited by an adversary. As such, the assurance of the availability of information through our networked forces becomes a vital consideration for the successful implementation of these network centric concepts.

INFORMATION ASSURANCE CONSIDERATIONS

Information Assurance is "the process for protecting and defending information by ensuring its confidentiality, integrity, and availability."[21] Army Regulation 25-2, *Information Assurance*, amplifies the definition of IA as, "The protection of systems and information in storage, processing, or transit from unauthorized access or modification: denial of service to unauthorized users; or in the provision of service to authorized users. It also includes those measures necessary to detect, document, and counter such threats."[22] Further, it expands the scope of IA by designating it as "…the security discipline that encompasses COMSEC, INFOSEC, and control of compromising emanations (TEMPEST)."[23] In other words, IA is the

end-to-end protection of friendly information and the measures taken to detect and thwart hostile access and manipulation of that information.

The applicable document dictating DoD guidelines regarding IA is DoD Directive 8500.1. This directive "establishes policy and assigns responsibility under Section 2224 of title 10, United States Code, "Defense Information Assurance Program" to achieve Department of Defense information assurance through a defense-in-depth approach that integrates the capabilities of personnel, operations and technology, and supports the evolution to network centric warfare."[24] To be consistent with the global C4ISR Framework, and to support the aforementioned defense-in-depth approach and evolution to NCW capabilities, this policy directive states that "this combination produces layers of technical and non-technical solutions that: provide appropriate levels of confidentiality, integrity, authentication, non-repudiation, and availability; defend the perimeters of enclaves; provide appropriate degrees of protection to all enclaves and computing environments; and make appropriate use of supporting IA infrastructures, to include robust key management and incident detection and response."[25] As shown, IA encompasses a broad range of measures to ensure the protection, integrity, and availability of information across the entire domain of information technology (IT) operating environments. Given the sweeping nature of network enabled capabilities, it is clear that IA principles, practices, guidelines and policy are critical elements to maintaining, protecting and leveraging the power that NCO provides. It should also be clear that U.S. dependence, and therefore, inherently our allies' dependence on the integrity of our myriad networks and more specifically the information that is distributed across them is a key and critical target for our adversaries' mischief.

STRATEGIC IMPLICATIONS

So, is this much ado about nothing, or is information assurance of our existing and emerging network centric capabilities a strategic imperative? The NSS of September 2002 prescribes that "innovation within the armed forces will rest on experimentation with new approaches to warfare, strengthening joint operations, exploiting U.S. intelligence advantages, and taking full advantage of science and technology."[26] Network centric operations and our assurance of the integrity of the information being passed across our networks is embedded in the each of the domains listed. Additionally, the 2001 Quadrennial Defense Review (QDR), which was primarily prepared in advance of the attacks of 11 September 2001, indicates that "new information and communications technologies hold promise for networking highly distributed joint and combined forces and for ensuring that such forces have better situational

awareness, both about friendly as well as those of adversaries, than in the past."[27] Both of these documents recognize the need to take advantage of U.S. technological superiority in IT capabilities across the full spectrum of operations and that our ability to employ NCO across that spectrum is significant to realizing national policy objectives.

To refine that thought further, it is instructive to consider the implied and derived implications that are captured in DoD policy and strategy directives that flow from the documents quoted above. The 2004 NMS specifically references the complex environment that joint and combined operations will be conducted in and indicates that "joint forces operating in this complex battlespace must be fully integrated and adaptable to anticipate and counter the most dangerous threats."[28] Recognizing the need not only for information superiority, but the requisite decision superiority that is necessary to provide a tactical, operational or strategic edge to the decision-maker, it further goes on to illustrate that "a networked force capable of decision superiority can collect, analyze, and rapidly disseminate intelligence and other relevant information from the national to the tactical levels, then use that information to decide and act faster than opponents."[29] To support joint force operations, the NMS further details the criticality of information assurance to the achievement of military objectives supporting the national security objectives. In order to ensure freedom of action within all domains of the battlespace, including cyberspace, it indicates that "military operations require information assurance that guarantees access to information systems and their products and the ability to deny adversaries access to the same. "[30] It further goes on to describe that "securing the battlespace includes action to safeguard information and command and control systems that support the precise application of force and sustainment activities that ensure persistence across the full range of military operations. Securing battlespace ensures the ability of the Armed Forces to collect, process, analyze and disseminate all-source intelligence and other relevant information that contribute to decision superiority."[31] Network centric operations, and the assurance that information disseminated across the networks is uncompromised, is considerable towards addressing this aim.

It should be apparent that NCW and NCO, and the expectation of the uncompromised fidelity of the information being passed through these networks, is a significant enabler, or in the National Strategy construct, one of our "ways" to facilitate the accomplishment of United States' National Security objectives. It should also be apparent that the inherent power that is provided by this particular type of advantage makes it an equally attractive target to our adversaries who would look to exploit it to their ends.

ONE MAN'S STRENGTH IS ANOTHER MAN'S VULNERABILITY

So, what are the challenges for Information Assurance in the Network Centric context? Additionally, what are some of the key vulnerabilities and threats associated with network centric forces and the proposed mitigation strategies to address them?

First, it is instructive to note that the QDR recognizes the general vulnerability in the following way, "The increasing dependence of societies and military forces on advance information networks creates new vulnerabilities through means such as computer network attack and directed energy weapons."[32] The inherent implication here is that the universal nature of networked systems is in and of itself one of the key vulnerabilities. Networks are pervasive, throughout almost every domain of both our civilian and military sectors, and have commensurately evolved into a critical essence amongst our various elements of power. As a result, they are attractive asymmetric targets to adversaries who do not have force equality in the traditional sense, but like much of the civilized world, have ready access to the Internet, as well as less sophisticated kinetic weapons (e.g., bombs, explosive materials, small arms, etc.) and can use that to asymmetric advantage.

Secondly, the fact that military networks and civilian networks commingle provides another vulnerability that must be addressed by IA strategies. The networked C4ISR infrastructure that connects tactical, operational and strategic nodes is only as secure as its weakest link.[33] Therefore, some of the power that is inherent in the reachback capability of networks to the sustaining base or to the overarching Global Information Grid (GIG) provides another attack opportunity for the asymmetric adversary. The GIG is the "globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel,"[34] It is the most ubiquitous of networks, and therefore, provides both the most power and the greatest vulnerability. Given that it transports and processes data, voice, video, and imagery at the full range of classification levels, the IA challenge is further complicated.

Third, even though the inherent nature of networks, and indeed, the networking function of each element in the network, provides additional robustness and redundancy, as noted earlier, there are still nodes within the network that are more critical than others. These nodes are created for a variety of reasons including increased dependence on civilian telecommunications infrastructure, use of commercial off-the-shelf (COTS) technologies in military hardware and software systems, and even a trend for the commercial sector, who as noted above, provide a certain portion of the DoD's telecommunications products, to outsource the development and

production of IT hardware and software to foreign vendors. This provides the potential opportunity for introduction of embedded functions in IT systems, and thus the network, that could have the ability to exploit or degrade overall system performance. If an adversary can identify and attack these critical nodes, they can potentially degrade the entire network; therefore, attacks against these critical nodes have the potential of producing a disproportionate effect on the overall performance and health of the network function.[35]

Ultimately, threats to network centric capabilities can include a wide variety of both domestic and international operatives including hackers, terrorists or state sponsored actors intent on disrupting operations, corrupting data, stealing sensitive information, denying network access, or exploiting network vulnerabilities.[36] Additionally, some threats are self-generated due to lack of diligence regarding our NCO enabling technologies or practices. Specific threats can fundamentally be lumped into the following categories - physical attack against critical nodes, electromagnetic attack against network nodes or elements, cyber attack against computer-based or IT systems within the network, and self-inflicted wounds; i.e., unintentional or inadvertent consequence to networks due to friendly actions or network failures.[37] The next section will examine these threats to NCW and NCO and provide suggested strategies to address or mitigate these threats.

PHYSICAL ATTACK AGAINST CRITICAL NODES

As noted in the previous section, physical attack of critical nodes and infrastructure remains one of the asymmetric avenues for adversaries to exploit in the NCO/NCW environment. Given that facilities and systems comprising these nodes and infrastructure exist both domestically and on foreign soil, these types of attacks can be implemented in traditional war-making ways or less sophisticated methods such as use of explosives or limited attack to achieve the desired disruptive or destructive effect.

One of the enabling necessities of NCO and NCW is the requirement for “reachback” of networked forces through the GIG to the sustaining base. Today, this is typically accomplished via satellite communications systems and other critical nodes that provide beyond line-of-sight, high-bandwidth capabilities and means. As recently as 2001, over 95 percent of telecommunications vital to our national security traveled over commercial telecommunications networks.[38] Therefore, attack of the facilities and systems that comprise this communications and information backbone is an attractive asymmetric target for our adversaries.

Additionally, attack of the infrastructure that provides basic support services, including electricity, water and transportation, has the potential for direct or indirect impact on

performance of the critical nodes, and thus, the overall network. Attack of these support services and the nodes that they service has substantial potential to have a disproportionate effect on network-enabled military operations.

Strategies to address these potential vulnerabilities include:

- Replication or redundancy of critical nodes or infrastructure. Although this must be done selectively do to fiscal reality, single points of failure, especially of critical nodes, must be minimized in the overall network architecture to reduce vulnerability to attack of any single critical node.
- Independent "Red Team" assessment of end-to-end vulnerabilities and interdependencies across the network. Use of modeling and simulation techniques to continually assess infrastructure and nodal vulnerabilities are essential to generating specific defenses against those vulnerabilities.

ELECTROMAGNETIC ATTACK

The threats to NCO in this realm cover a range of possibilities from directed energy (DE) and high-power radio frequency (RF) weapons to electronic warfare (EW) to everyone's favorite, nuclear explosion generated electromagnetic pulse (EMP). These types of threats have the potential to degrade or otherwise incapacitate elements of a network or critical nodes without specific kinetic attack or effects.

Directed energy and high power RF weapons are generally reserved for the more developed and sophisticated adversary, although there are commercially available technologies that could allow the state-sponsored or rogue actor to develop rudimentary capability in this domain. In this realm, ground-based, high-energy lasers can be used to blind or disable satellite-based sensors and high-power RF weapons can be used to create a wide range of effects, from upsetting electronics to destroying them in both military and commercial applications feeding network-centric systems.[39]

Another form of high-energy threat is nuclear detonation generated EMP. This type of EMP can produce large electric fields over a significant area, dependent on the altitude of detonation, and poses a significant threat to electronic systems.[40] Measures can be taken to "harden" systems and electronics against EMP, but there is significant cost associated with implementing these and as a result, many systems have limited or no protection against EMP effects. On the upside, the general threat of an air or space detonation of an EMP-generating nuclear weapon is considered low, so EMP-mitigating measures should always be implemented accordingly.

Finally, EW is the form of electromagnetic attack that is generally associated with the "jamming" of sensors, command and control, or communications systems that are also using the electromagnetic spectrum. Although communications systems remain one of the key targets to EW jamming methods, systems such as the Global Positioning System (GPS), a vital contributor to NCO-enabled concepts such as situational awareness/understanding and the common operational picture (COP), have emerged as important objectives to an EW campaign.

Information assurance mitigation strategies to address these threats include:

- Hardening of important sensor and C3 electronics. Such hardening is expensive and comes with a weight penalty, thus its implementation must be done judiciously
- Use of directional antennas, "spot beams"[41] and higher power downlinks on satellite-based systems. These methods provide for increased gain in the main lobe of the downlink and are an inherent defense against both intentional and unintentional electromagnetic interference.
- Focused intelligence collection on adversaries' capabilities in this area of concentration. Because of the potential for significant deleterious effects on a wide range of important communications and electronics assets, this must remain an area of priority intelligence collection.

INFORMATION WARFARE

Cyber attack, or Information Warfare (IW), remains one of the most attractive, troublesome and pervasive avenues of asymmetric attack against network centric systems. Because the use of computers and processors in every weapon's platform is inescapable and the ready availability of computer technology to all potential adversaries is assured, this threat is highly problematic. Investment in cyber warfare resources is minimal, information regarding hacking techniques is readily available, and threat to the hacker of being identified or captured is relatively low. IW methods and techniques truly provide for asymmetric warfare and disproportionate effects on NCO capabilities.

Documented instances of computer intrusion by the Computer Emergency Response Team (CERT) Coordination Center continue to rise dramatically from approximately 21,756 reported in 2000, to 52,658 in 2001, and 82,094 in 2002, and 137,529 in 2003.[42] More alarming is the fact that CERT estimates that only ten percent of such attacks are detected, and fewer still are reported.[43] The United States is susceptible to such attacks because it is highly dependent upon computer networks for many essential services, but has not adequately addressed the computer network attack threat.[44]

Every day in the United States, hundreds and sometimes thousands of unauthorized attempts are made to breach computer systems supporting critical military and commercial nodes and infrastructure – defense facilities, government agencies, power grids, and telecommunications and transportation networks. Although most are not successful, some are, and potentially allow intruders to gain system administrator privileges, download passwords, implant "sniffers" to copy transactions, or trap doors to permit an easy return. While some attacks are done just for sport, some are more insidious in their intent, collecting intelligence, inserting viruses, or providing the means for a future attack capability. [45] Significantly, these are likely to increase in sophistication and frequency as the U.S. moves towards a fully net-centric force.

Mitigation strategies to address these include:

- Improved network monitoring, intrusion detection software and algorithms. These broad system administration functions remain vital to preventing unauthorized access and transit within the network. Comprehensive initial and recurring training of system administrators as to the full capabilities and intended implementation of these tools is an essential complementary aspect to achieve full effectiveness of this strategy.
- Advanced software firewalls and encryption algorithms. As reliance on both enterprise and operational-level computer networks continues to grow, industry and the DoD must continue to invest in these two areas as part of its layered defense strategy to network IA. Again, a robust and recurring training regimen is essential to the desired efficacy of these measures. Additionally, closer cooperation between network administrators and those administering the firewalls is crucial to ensuring the intended protection of the products or algorithms.
- Physical separation of critical networks from less secure potential sources of intrusion. This will continue to remain one of the best ways to ensure the fidelity of the information being passed within the network; however, it comes at the potential price of greater overall network connectivity and must be implemented accordingly.

SELF-INFLICTED WOUNDS

The final area of consideration with respect to information assurance considerations for NCO and NCW focuses on those actions, or inactions, taken by friendly forces that result in network disruptions or random, unintended failures of the network that have deleterious effects on network operations and performance. These kinds of events have the same deleterious

effects on network operations and performance as if they had been carried out by our adversaries.

One source of these unintended disruptions is caused by improper network administration. These types of network disruptions are attributable to insufficient training of network or system administration personnel and are responsible for over 30 percent of network outages or degradation.

Another source of network degradation is caused by random event upsets within the network, complexity of system interactions, or network software crashes. These are usually not predictable and can potentially have the effect of bringing the network to its knees. The random nature of such failures provides another source of confusion to network administrators and monitors trying to assess whether the source of failure is due to a malicious intrusion of or natural event upset.

Strategies to address these deficiencies or unintended network vulnerabilities include:

- Better monitoring of IT software and hardware development and implementation. Of all the strategies listed, this has the potential for greatest pay-off. Rather than the field and patch mentality that currently exists with respect to these efforts, the acquisition process should emphasize and incentivize up-front development of IT products that conform to a common set of robust and testable IA standards. This will serve to reduce overall network vulnerability to exploitation and the IA burden on the network administration function.
- In-depth, more robust training of network administrators. Rather than the ad hoc process that exists today, network administrators should be trained to a common standard throughout the DoD by means of an institutionalized and universally accepted certification process. This will contribute to a greater proficiency across the DoD information technology domain of network administration and monitoring capability and a reduction of self-induced network disruptions and vulnerabilities.
- Built-in redundancy for critical network elements. Similar to radiation hardening of electronics, this particular strategy adds additional cost to development and implementation of the overall network, but is appropriate to protect network elements whose compromise or destruction would have disproportionate effects on overall network health or function.
- A rapid reconstitution capability subsequent to system outages. Given that unforeseen network upsets and system outages are inevitable, networks must be developed and configured with an eye towards rapid recovery from such disruptions.

FINAL RECOMMENDATIONS

It is clear that IA strategies and policies must be religiously enforced and updated to counter the threat to our increasing dependence on network centric operations. These strategies are complex and require constant attention and update to assure information flow and fidelity across the full spectrum of operations. The following recommendations are viewed as providing the highest return on investment with respect to information assurance of NCO and network enabled forces:

1) Red Teams – These should be used extensively and early in the developmental cycle of new C3 systems and the platforms on which they are integrated. Findings from these Red Teams can then be flowed back into the DOTLMP-F cycle and incorporated into the appropriate production or pre-production models prior to fielding of systems. Additionally, the Red Team construct should be applied against existing networks to confirm the fidelity and robustness of the information flow across the network, and provide feedback to network administrators for implementation in system administration function and upgrades.

2) Tougher standards and monitoring for software and hardware builds – Outsourcing of electronic hardware and network software, whilst an accepted and pervasive practice in industry, has the potential to introduce hidden, embedded, and potentially even malicious undetected software and instruction sets in DoD systems. As such, industry should be incentivized, either positively or negatively, to ensure software security best practices and closer monitoring of their sub-vendors. This should be institutionalized within the DoD Acquisition Process and emphasized at the highest levels within DoD.

3) Selective Hardening – Critical nodes and elements within the networked systems should be identified as such and be subjected to higher standards for hardening against natural and man-made sources of directed energy or high-power RF. Additionally, where feasible, sensor and communications systems that are distributed, use spatially dispersed elements and links, and robust software algorithms that can tolerate and compensate for failed delivery of messages and packets should be incorporated into the network design.

4) Better training for network administrators – Given the amount of operator induced network outages, great care and attention should be given to ensuring a minimum degree of competence and understanding regarding network operations to include a full certification process under the direction and administration of a single DoD entity. Logical administration of this effort would be under the purview of the Joint Staff J6, with assistance and oversight from the Assistant Secretary of Defense for Networks and Information Integration, ASD(NII).

CONCLUSION

This paper has attempted to outline the importance of information assurance within the context of network centric warfare and operations, not only as an important enabler to Army transformation, but as a strategic imperative towards meeting our national objectives. Network centric operations are a key element of force transformation and will continue to be so for the foreseeable future. As such, protection of these networks and assurance of the information being passed across them is critical to maintaining the warfighting advantage that they provide.

This paper has examined some of the key threats facing network centric forces and the commensurate methodologies necessary to achieve the promise of NCO and NCW capabilities. In particular, the areas of physical attack against critical nodes, electromagnetic attack against network nodes or elements, cyber attack against computer-based or IT systems within the network, and unintentional or inadvertent consequence to networks due to friendly actions or network failures were looked at in detail and mitigation strategies proffered address these threats or vulnerabilities.

Finally, specific recommendations were provided to suggest high pay-off areas of focus for implementation in existing and future programs and processes to facilitate successful network centric systems and operations. To realize the full promise of information-age and transformational capabilities, it is clear we will need to practice due diligence to ensure the fidelity of the data being shared amongst the collective constituents that comprise the joint force of the future.

WORD COUNT=5938

ENDNOTES

[1] Donald Rumsfeld, *Transformation Planning Guidance* (Washington, D.C.: Office of the Secretary of Defense, April 2003),

[2] David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority* 2nd ed. (Washington, DC: CCRP Publication Series, February 2000), 88.

[3] Department of the Army, *Army Vision 2010*, (Washington D.C.; Department of the Army), 1.

[4] Roger Roberts, "Network Centric Operations", Speech given at the Network Centric Operations 2003 Conference, 2003, Apr 16 2003, available from <http://www.boeing.com/news/speeches/2003/Roberts_030416.html>; Internet, accessed 12 October 2004.

[5] Ibid.

[6] Ibid.

[7] Department of Defense, *Network Centric Warfare, Report to Congress*, iv.

[8] Joint Chiefs of Staff, Joint Vision 2020, (Washington, D.C.: Joint Staff, J-5, June 2000), 11.

[9] Robert K. Ackerman, "Challenges Loom for Network-Centric Warfare," *Signal Magazine*, November 2001; available from < http://www.afcea.org/signal/articles/anmviewer.asp?a=477>; Internet; accessed 21 February 2005.

[10] Office of the Secretary of Defense, *Joint Operations Concepts*, (Washington, D.C.: Office of the Secretary of Defense, November 2003), 3.

[11] Training and Doctrine Command, *Joint Concepts Summaries*, (Fort Monroe, VA: TRADOC Futures Center, 27 Feb 03), 4.

[12] Ibid.

[13] Office of the Secretary of Defense, *Joint Operations Concepts*, 15.

[14] Ibid.

[15] Office of the Secretary of Defense, *Military Transformation: A Strategic Approach*, (Washington, D.C.: Office of Force Transformation, Fall 2003), 34.

[16] Ibid.

[17] U.S. Department of the Army, *2003 United States Army Transformation Roadmap* (Washington, D.C.: U.S. Department of the Army, November 2003), p. II.

[18] Ibid, p. 1-7.

[19] Office of the Secretary of Defense, *The Implementation of Network Centric Warfare*, (Washington, D.C.: Director, Force Transformation, 5 January 2005), 51.

[20] This statement was made at an FCS program review in January 2004.

[21] Joseph G. Boyce and Dan W. Jennings, *Information Assurance*, (Woburn, MA: Elsevier Science, 1 June 2002), 3.

[22] Department of the Army, AR 25-2, *Information Assurance*, (Washington, D.C.: HQ, Department of the Army, 14 Nov 2003), 73.

[23] Ibid; COMSEC is Communications Security, INFOSEC is Information Security, and TEMPEST is Transient Electromagnetic Pulse Emanation Standard.

[24] Office of the Secretary of Defense, *DoD Directive 8500.1*, (Washington, D.C.: ASD(C3), 24 October 2002), 1.

[25] Ibid, 4.

[26] Bush, George W., *The National Security Strategy of the United States of America*, (Washington, D.C.: The White House, September 2002), 30.

[27] Department of Defense, *Quadrennial Defense Review Report,* (Washington, D.C.: Department of Defense, 30 September 2001), 31.

[28] Department of Defense, *National Military Strategy of the United States of America*, (Washington, D.C.: Department of Defense, 2004), 14.

[29] Ibid.

[30] Ibid, 17.

[31] Ibid.

[32] Department of Defense, *Quadrennial Defense Review Report*, 31.

[33] Carl D. Porter, *Network Cenric Warfare: Transforming the U.S. Army,* (Carlisle Barracks: U.S. Army War College, 19 March 2004), 12.

[34] Joint Chiefs of Staff, *Enabling the Joint Vision,* (Washington, D.C.: Department of Defense, Joint Staff, C4 Systems Directorate, May 2000), 12.

[35] Jacques S. Gansler and Hans Binnendijk, *Information Assurance: Trends in Vulnerabilities, Threats, and Technologies*, Working Paper, (Washington, D.C.: Center for Technology and National Security Policy, May 2004), 17.

[36] Porter, 12.

[37] Gansler and Binnendijk, 19.

[38] Donald H. Rumsfeld, “Report of the Commission to Assess United States National Security Space Management and Organization,” 11 January 2001, available from <http://www.defenselink.mil/pubs/space20010111.html>; Internet; accessed 21 February 2005.

[39] Eileen Walling, *High Power Microwaves: Strategic and Operational Implications for Warfare*, Occasional Paper No. 11 (Maxwell AFB, AL: Center for Strategy and Technology, Air War College, May 2000), 2.

[40] Kenneth R. Timmerman, “U.S. Threatened with EMP Attack,” Investigative Report, 28 May 2001, 16.

[41] Spot beams are used on communications satellites to provide higher gain over a reduced geographic footprint.

[42] Statistics as reported by the CERT Coordination Center. Available from <http://www.cert.org/stats/cert_stats.html#incidents>; Internet; accessed 1 Mar 2005.

[43] Ibid.

[44] Mark D. Baines, *The National Telecommunications Infrastructure: A 21st Century Paradox*, Strategy Research Project (Carlisle Barracks: U.S. Army War College, April 2003), 3.

[45] Ibid.

BIBLIOGRAPHY

Ackerman, Robert K. "Challenges Loom for Network-Centric Warfare." November 2001. Available from < http://www.afcea.org/signal/articles/anmviewer.asp?a=477>. Internet. Accessed 21 February 2005.

Alberts, David S., John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority* 2nd ed. Washington, DC: CCRP Publication Series, February 2000.

Boyce, Joseph G. and Dan W. Jennings, *Information Assurance*. Woburn, MA: Elsevier Science, 1 June 2002.

Bush, George W. *The National Security Strategy of the United States of America*. Washington, D.C.: The White House, September 2002.

Bush, George W. *The National Strategy for Homeland Security*. Washington, D.C.: The White House, July 2002.

Bush, George W. *The National Strategy to Secure Cyberspace*. Washington, D.C.: The White House, February 2003.

Cebrowski, Arthur K. and John J. Gartska. "Network Centric Warfare: Its Origin and Future." *Naval Institute Proceedings*, Annapolis: U.S. Naval Institute, 1998.

CERT Coordination Center. "Statistics, 1988-2004." Available from <http://www.cert.org/stats/cert_stats.html#incidents>. Internet. Accessed 1 Mar 2005.

Gansler, Jacques S. and Hans Binnendijk, *Information Assurance: Trends in Vulnerabilities, Threats, and Technologies*. Washington, D.C.: Center for Technology and National Security Policy, National Defense University, May 2004.

Joint Chiefs of Staff, *Enabling the Joint Vision.* Washington, D.C. Department of Defense, Joint Staff, C4 Systems Directorate, May 2000.

Joint Chiefs of Staff, *Joint Vision 2020*. Washington, D.C. Joint Staff, J-5, June 2000.

Joint Chiefs of Staff. *National Military Strategy of the United States of America*. Washington, D.C.: U.S. Joint Chiefs of Staff, 2004.

Office of the Secretary of Defense. *Information Assurance*. DoD Directive 8500.1. Washington, D.C. Assistant Secretary of Defense for Command, Control, Communications and Intelligence, 24 October 2002.

Office of the Secretary of Defense. *Information Assurance Implementation*. DoD Instruction 8500.2. Washington, D.C. Assistant Secretary of Defense for Command, Control, Communications and Intelligence, 6 February 2003.

Office of the Secretary of Defense, *Joint Operations Concepts*. Washington, D.C.: Office of the Secretary of Defense, November 2003.

Office of the Secretary of Defense, *The Implementation of Network Centric Warfare*. Washington, D.C. Director, Force Transformation, Office of the Secretary of Defense, 5 January 2005.

Olsen, Florence. "From Layers to Assurance." 18 February 2005; available from <http://www.fcw.com/fcw/articles/2005/0214/web-assurance-02-18-05.asp>. Internet. Accessed 21 February 2005.

Porter, Carl D. *Network Centric Warfare: Transforming the U.S. Army*. Strategy Research Project. Carlisle Barracks: U.S. Army War College, 19 March 2004.

Roger Roberts, "Network Centric Operations", Speech given at the Network Centric Operations 2003 Conference, 2003, Apr 16 2003, available from <http://www.boeing.com/news/speeches/2003/Roberts_030416.html>; Internet, accessed 12 October 2004.

Rumsfeld, Donald, *Transformation Planning Guidance*. Washington, D.C.: Office of the Secretary of Defense, April 2003.

Sarkar, Dibya. "DHS Buys Information Assurance." 27 December 2004. Available from <http://www.fcw.com/fcw/articles/2004/1227/web-qradar-12-27-04.asp>. Internet. Accessed 21 February 2005.

Tibboni, Frank. "DoD fights 'Net." 21 January 2005. Available from <http://www.fcw.com/fcw/articles/2005/0117/web-wolf-01-21-05.asp>. Internet. Accessed 21 February 2005.

Timmerman, Kenneth R. "U.S. Threatened with EMP Attack." *Investigative Report*, 28 May 2001.

U.S. Army Training and Doctrine Command, *Joint Concepts Summaries*. Fort Monroe, VA: U.S. Army TRADOC Futures Center, 27 Feb 03.

U.S. Department of the Army, *Army Vision 2010*. Washington, D.C.: U.S Department of the Army.

U.S. Department of the Army, Army Regulation 25-2, *Information Assurance*. Washington, D.C.: HQ Department of the Army, 14 November 2003.

U.S. Department of the Army, *2003 United States Army Transformation Roadmap*. Washington, D.C.: U.S. Department of the Army, November 2003.

U.S. Department of Defense, *Quadrennial Defense Review Report*. Washington, D.C.: Department of Defense, 30 September 2001.

Walling, Eileen M. "High Power Microwaves: Strategic and Operational Implications for Warfare." Maxwell AFB, AL: Center for Strategy and Technology, Air War College, 1999.